WHAT IS CLAIMED IS:

1. An access control method for verifying a user's access to a network, comprising the steps:

upon receiving an indication signifying that said user is attempting to access said network using a multimedia appliance, invoking a multimedia session engine to launch a network access application;

interrogating said user by an access application server associated with said network;

receiving a multimedia response from said user responsive to said interrogating step;

determining if said multimedia response is valid; and

if so, granting permission to said user with respect to accessing said network.

2. The access control method for verifying a user's access to a network as set forth in claim 1, wherein said user is remotely located with respect to said network.

3. The access control method for verifying a user's access to a network as set forth in claim 2, wherein said multimedia response from said user comprises an audio response responsive to said interrogating step.

4. The access control method for verifying a user's access to a network as set forth in claim 2, wherein said multimedia response comprises a video input of said user in response to said interrogating step.

5. The access control method for verifying a user's access to a network as set forth in claim 4, wherein said video input comprises a live picture of said user.

6. The access control method for verifying a user's access to a network as set forth in claim 2, further comprising the steps:

upon granting permission to said user with respect to accessing said network, re-interrogating said user after a time period;

receiving a response from said user responsive to said re-interrogating step; and

if said response from said user not valid, terminating said user's access to said network.

7. The access control method for verifying a user's access to a network as set forth in claim 6, wherein said response from said user comprises at least one of an audio response, a video input, a device input effectuated via said multimedia appliance, and a biometric ID input of said user.

8. The access control method for verifying a user's access to a network as set forth in claim 7, wherein said network comprises a corporate computer network, and further wherein said re-interrogating step is effectuated by a human operator associated with said corporate computer network.

9. The access control method for verifying a user's access to a network as set forth in claim 7, wherein said network comprises a corporate computer network, and further wherein said re-interrogating step is effectuated by an automated access control apparatus associated with said corporate computer network.

10. The access control method for verifying a user's access to a network as set forth in claim 7, wherein said network comprises a home network, and further wherein said re-interrogating step is effectuated by an access control application server associated with a public network that serves said user.

11. An access control system for use with a multimedia-capable next-generation network, said system for providing remote access to a network portion, comprising:

means for receiving an indication signifying that a remotely located user is attempting to access said network portion using a multimedia appliance;

a multimedia session engine operable to invoke a network access application, responsive to said indication, on an access application server associated with said multimedia-capable next-generation network;

means for interrogating said remotely located user for a multimedia response, said means for interrogating operating responsive to control inputs provided by said multimedia session engine;

logic means, associated with said access application server, for determining if said multimedia response form said user is valid; and

means for granting permission to said user with respect to accessing said network portion, provided said multimedia response has been determined to be valid.

12. The access control system for use with a multimedia-capable next-generation network as set forth in claim 11, wherein said network portion comprises a network selected from the group consisting of a corporate network, a home network, a small business network, and a private enterprise network.

13. The access control system for use with a multimedia-capable next-generation network as set forth in claim 12, wherein said multimedia response comprises at least one of an audio response, a video input, a device input effectuated via said multimedia appliance, and a biometric ID input of said user.

14. The access control system for use with a multimedia-capable next-generation network as set forth in claim 13, further including means for re-interrogating said remotely located user after a select time period upon granting permission to access said network portion.

15. The access control system for use with a multimedia-capable next-generation network as set forth in claim 13, wherein said means for interrogating said remotely located user includes means for effectuating different levels of interrogation depending upon a plurality of access levels allowed with respect to said network portion.

16. A computer-accessible medium operable with a network element disposed in a multimedia-capable next-generation network, said computer-accessible medium carrying a sequence of instructions which, when executed by at least one processing entity associated with said multimedia-capable next-generation network, cause said network element to perform the following steps:

upon receiving an indication signifying that a user is attempting to access a network portion using a multimedia appliance, invoking a multimedia session engine to launch a network access application;

directing an access application server associated with said multimedia-capable next-generation network to interrogate said user;

receiving a multimedia response from said user responsive to said interrogating step;

determining, in said access application server, if said multimedia response is valid; and

if so, granting permission to said user with respect to accessing said network portion.

17. The computer-accessible medium operable with a network element disposed in a multimedia-capable next-generation network as set forth in claim 16, wherein said network portion comprises a network selected from the group consisting of a corporate network, a home network, a small business network, and a private enterprise network.

18. The computer-accessible medium operable with a network element disposed in a multimedia-capable next-generation network as set forth in claim 17, wherein said user is remotely located with respect to said network portion.

19. The computer-accessible medium operable with a network element disposed in a multimedia-capable next-generation network as set forth in claim 18, wherein said multimedia response comprises at least one of an audio response, a video input, a device input effectuated via said multimedia appliance, and a biometric ID input of said user.

20. The computer-accessible medium operable with a network element disposed in a multimedia-capable next-generation network as set forth in claim 19, wherein said sequence of instructions further includes instructions to carry out the following steps:

upon granting permission to said user with respect to accessing said network portion, re-interrogating said user after a time period;

receiving a response from said user responsive to said re-interrogating step; and

if said response from said user not valid, terminating said user's access to said network portion.

21. A user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility, comprising the steps of:

upon receiving an indication that said user is attempting to access said controlled facility, invoking a multimedia session engine to launch an access service application;

interrogating said user by an access application server associated with said service network;

receiving a multimedia response from said user responsive to said interrogating step;

determining if said multimedia response is valid; and

if so, granting permission to said user with respect to accessing said controlled facility in accordance with a user access profile stored on said service network.

22. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 21, wherein said multimedia response from said user comprises at least one of an audio response, video response, and a text response, and further wherein said controlled facility is selected from the group consisting of a corporate network, a home network, a physical area, and an access-controlled service.

23. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, further comprising the steps:

upon granting permission to said user with respect to accessing said controlled facility, re-interrogating said user after at least one of a predetermined time period and a predetermined user action;

receiving a response from said user responsive to said re-interrogating step; and

if said response from said user not valid, terminating said user's access to said controlled facility.

24. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, wherein said audio response comprises playing back on a multimedia appliance a stored audio file associated with said user.

25. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, wherein said audio response comprises generating a live audio file associated with said user on a multimedia appliance.

26. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, wherein said video response comprises playing back on a multimedia appliance a stored video file associated with said user.

27. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, wherein said video response comprises generating a live video file associated with said user on a multimedia appliance.

28. The user verification method for use in a service network for positively identifying a user attempting to gain access to a controlled facility as set forth in claim 22, wherein said multimedia response further includes providing a still photograph of said user.